ЦАРЕГОРОДЦЕВ А. В., ЛОГИНОВА А. О., БЛОХИНА О. В.

МЕТОДИКА КОЛИЧЕСТВЕННОЙ ОЦЕНКИ РИСКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ОБЛАЧНОЙ ИНФРАСТРУКТУРЫ ОРГАНИЗАЦИИ

Аннотация. В связи с тем, что облачные вычисления несут новые вызовы в области информационной безопасности, для организации крайне важно контролировать процесс управления информационными рисками в облачной среде. В статье предложен подход к оценке рисков, используемый при выборе наиболее приемлемого варианта конфигурации среды облачных вычислений с точки зрения требований безопасности.

Ключевые слова: облачные вычисления, угрозы информационной безопасности, анализ информационных рисков, методы управления информационной безопасностью, требования информационной безопасности.

TSAREGORODTSEV A. V., LOGINOVA A. O., BLOKHINA O. V.

DATA SECURITY RISK ASSESSMENT FOR CLOUD INFRASTRUCTURE OF ORGANIZATION

Abstract. Due to the fact that cloud computing brings about new challenges for information security, it is imperative for organizations to control the process of information risk management in a cloud. This paper proposes a risk assessment approach used for the selection of the most appropriate configuration options of cloud computing environment from the point of view of security requirements.

Keywords: cloud computing, information security threats, information risk analysis, information security management tools, information security requirements.

Одной из серьезных угроз информационной безопасности (ИБ) облачных сред является использование со стороны злоумышленников известных, но не исправленных уязвимостей [4]. Успешная реализация эксплойта потенциально может привести к значительному финансовому ущербу для клиента, потере репутации облачного провайдера и компрометации используемых механизмов защиты [2].

Принимая во внимание тот факт, что поддержка конфигурации облачной среды, управление уязвимостями и обновлениями зависит от модели предоставления облачного сервиса, ответственность за своевременное выполнение этих задач частично или полностью лежит на стороне облачного провайдера [7].

В этом случае одной из основных задач обеспечения ИБ информационных систем (ИС) становится рассмотрение и классификация уязвимостей облачных сред и возможность использования этой информации при проведении количественной оценки риска.

Предлагаемая методика позволит принять решение при выборе систем защиты информации, программного обеспечения для компонентов ИС, функционирующей на основе технологии облачных вычислений.

Основные этапы методики количественной оценки риска.

Для возможности проведения количественной оценки и построения риск-модели облачной среды необходимо решить следующие задачи.

1. Определить и описать возможные технические риски использования облачных сред в их взаимосвязи с уязвимостями и активами организации.

2. Сформировать перечень уязвимостей для каждого риска, построить для них базовые векторы системы общего учета уязвимостей (CVSS).

3. Разработать методику по оценке уровня риска. Показатели частоты и урона будут рассчитываться на основе показателей CVSS метрик: базовой, временной и инфраструктурной.

4. Определить риск-модель на основе полученных уровней влияния рассматриваемых уязвимостей. Группировка уязвимостей по принципу принадлежности одному уровню влияния позволит ввести новый показатель – сервисный уровень. Совокупное представление возможных сервисных уровней и интенсивности переходов между ними позволит прогнозировать уровни риска в определенный момент времени.

Представим методику оценки рисков в виде следующих связанных процессов/действий: идентификация контекста оценки риска, идентификация риска, анализ риска, оценивание риска, обработка риска (рис. 1).

На верхнем уровне предлагаемая методика по оценке рисков включает два основных этапа. Первый этап описывает управляемый риском анализ, который включает оценивание набора злонамеренных использований и связанных с ними уровней риска, которые являются результатом шагов 2, 3, 4 описанной методики с последующим сравнением полученных значений с критериями принятия риска, которые определены на шаге 1. Результатом этой фазы является набор рисков, требующих обработки [9; 10].

Набор рисков для обработки, набор альтернативных решений и других компромиссных параметров, соответствующих разработке, проекту и финансовому состоянию являются входными данными для второго этапа методики.

Рис. 1. Методика оценки риска.

Действия, описанные в рамках первого этапа, включают ключевые элементы анализа: набор угроз, уязвимости; злонамеренное использование, его частота и влияние; риск ИБ, критерии принятия риска. При этом риск рассчитывается для каждого злонамеренного использования путем комбинации его частоты с одним из влияний. Это означает, что злонамеренное использование приводит к появлению одного или нескольких рисков ИБ, зависящих от количества связанных влияний [8].

Частота злонамеренного использования и его влияние могут быть представлены в виде количественных показателей: определенное количество проявлений в течение временного интервала или вероятность появления злонамеренного использования в

определенный период времени. Влияние может быть представлено в виде финансовых потерь, потери репутации и т. д. [1; 3]. Статистические ожидаемые потери =

$$= (I_1 \times F_1) \times L_1 + (I_i \times F_i) \times L_i + \cdots + (I_n \times F_n) \times L_n\} \quad (1)$$

Используя полученные выражения как базу для оценки, рассмотрим основные положения общей системы учета уязвимостей (CVSS), предоставим их характеристику и интерпретацию показателей применительно к среде облачных вычислений.

Основные положения общей системы учета уязвимостей. Общая система учета уязвимостей (CVSS) [6] в настоящее время достаточно широко применяется и все больше принимает вид стандарта для определения и оценки уязвимостей. Основная задача системы состоит в оценке уровня серьезности уязвимостей и предоставлении рекомендаций по смягчению последствий проявления угроз.

Показатели *базовой группы* описывают характеристики уязвимости, которые являются постоянными и не зависят ни от времени, ни от инфраструктуры. Основными показателями данной группы являются:

а) вектор доступа. Этот показатель отражает то, каким доступом должен обладать злоумышленник для эксплуатации уязвимости. Значения показателя и описание приведены в таблице 1;

б) сложность доступа. Этот показатель описывает сложность атаки, необходимой для эксплуатации уязвимости. Чем ниже уровень сложности, тем выше показатель уязвимости;

в) аутентификация. Показатель «Аутентификация» описывает количество необходимых сеансов аутентификации цели при эксплуатации уязвимости. Показатель не учитывает сложности этого процесса, а лишь характеризует саму необходимость аутентификации для использования уязвимости. Аутентификация происходит только в том случае, если доступ к ресурсу уже получен.

Расчет базовой метрики происходит следующим образом:

$$BaseScore =$$

$$= round\_to\_1\_decimal\{[(0{,}6 * Impact) + (0{,}4 * Exploitability) - 1{,}5] + f(Impact)\}, \quad (3)$$

где *BaseScore* – базовая метрика, *Impact* – общее влияние (урон), *Exploitability* – доступность использования эксплойта;

$$Impact = 10{,}41 * \big(1 - (1 - ConfImpact) * (1 - IntegImpact) * (1 - AvailImpact)\big), \quad (4)$$

где $ConfImpact$ – урон конфиденциальности, $IntegImpact$ – урон целостности, $AvailImpact$ – урон доступности;

$$Exploitability = 20 * AccessVector * AccessComplexity * Authentication, \quad (5)$$

где $AccessVector$ – вектор доступа, $AccessComplexity$ – вектор сложности, $Authentication$ – аутентификация; $f(impact) = 0,$ если $Impact = 0,$ в других случаях $f = 1,176.$

Временная метрика описывает показатели угрозы, реализующей рассматриваемую уязвимость. Метрика включает 3 показателя. Приведем краткое описание каждого из них.

А) Доступность кода и техники эксплойта. Этот показатель характеризует доступность и технику (код) эксплойта. Доступность в общедоступном доступе рабочего эксплойта (открытого кода) резко повышает количество потенциальных злоумышленников.

Б) Степень готовности решения для ликвидации последствий уязвимости. В общем случае уязвимость после ее появления в течение определенного времени не имеет исправлений в виде патча или официального обновления.

В) Степень достоверности информации об уязвимости. Этот показатель отражает степень достоверности источников о существования самой уязвимости, а также возможность использования технических деталей эксплойта.

Расчет временной метрики включает веса временных показателей с комбинацией с базовой оценкой, при этом результат находится в диапазоне от 0 до 10. Итоговая оценка временной метрики не превышает базовую оценку, но должна быть не меньше 33% от нее.

$$TemporalScore = round\_to\_1\_decomal\ (BaseScore * Exploitability * RemediationLevel * ReportConfidence), \quad (6)$$

где $TemporalScore$ – временная метрика, $BaseScore$ – базовая метрика, $Exploitability$ – доступность кода и техники эксплойта $RemediationLevel$ – степень готовности решения, $ReportConfidence$ – достоверность информации.

Метрики среды эксплуатации (инфраструктуры).

А) Сопутствующий потенциальный ущерб. Показатель описывает возможные потери (финансовые) в результате успешной эксплуатации уязвимости.

Б) Распределение целевых систем. Показатель описывает, какая часть компонентов облачной ИТКС подвержена уязвимости.

В) Требования к безопасности. Показатель позволяет специалисту ИБ определить приоритет и важность ключевых требований безопасности: конфиденциальность, целостность, доступность. Общий эффект инфраструктурного показателя зависит от соответствующих значений частных показателей из базовой метрики – урон для конфиденциальности, целостности и доступности. Расчет инфраструктурной метрики происходит следующим образом:

$$EnvironmentalScore = round\_to\_1\_decimal((AdjustedTemporal + (10 - AdjustedTemporal) * CollateralDamagePotential) * TargetDistribution), \quad (7)$$

где *EnvironmentalScore* – инфраструктурная метрика, *TargetDistribution* – распределение целевых систем, *CollateralDamagePotential* – сопутствующий потенциальный ущерб, *AdjustedTemporal* – скорректированная оценка временной метрики, пересчитанная с учетом требований безопасности и урона из базовой метрики ($AdjustedImpact$).

$$AdjustedImpact = \min(10{,}10{,}41 * (1 - (1 - ConfImpact * ConfReq) * (1 - IntegImpact * IntegReq) * (1 - AvailImpact * AvailReq))), \quad (8)$$

где $ConfReq$, $IntegReq$, $AvailReq$ – требования к конфиденциальности, целостности, доступности.

Таким образом, получается базовый, временной и инфраструктурный векторы, которые приведены в таблице 1.

Таблица 1

Показатели требований к безопасности

Группа метрик	Вектор
Базовая	AV:[L,A,N]/AC:[H,M,L]/Au:[M,S,N]/C:[N,P,C]/I:[N,P,C]/A:[N,P,C]
Временная	E:[U,POC,F,H,ND]/RL:[OF,TF,W,U,ND]/RC:[UC,UR,C,ND]
Инфраструктурная	CDP:[N,L,LM,MH,H,ND]/TD:[N,L,M,H,ND]/CR:[L,M,H,ND]/ IR:[L,M,H,ND]/AR:[L,M,H,ND]

Используя базовый, временной и инфраструктурный векторы определяются два основных интегральных показателя, влияющих на оценку риска. Чем выше уровень подверженности уязвимости применению эксплойта, тем больше шансов у злоумышленника провести успешную атаку и тем больше показатель *частоты злонамеренного использования* (*F*). Потенциальное влияние определяется как урон *(влияние),* зависящий от показателей уязвимости в базовой метрике и, в то же время, может быть увеличено или уменьшено в зависимости от требований к конфиденциальности, доступности и целостности, определенных в инфраструктурной метрике.

Анализ возможных угроз и анализ рисков служит основой для обоснования выбора мер по обеспечению ИБИС облачных вычислений, которые должны быть осуществлены для снижения риска до приемлемого уровня.

На базе общей системы оценки уязвимостей (CVSS), позволяющей определить качественный показатель подверженности уязвимостям с учетом факторов окружающей среды, была разработана методика количественной оценки потенциальных уязвимостей для различных типов развертывания облачных сред.

Предложенный подход к анализу и управлению рисками позволяет провести оценку защищенности облачной среды, функционирующей в условиях воздействия рассматриваемого класса угроз, а также эффективности комплекса мер и средств противодействия этим угрозам. На основе полученной оценки появляется возможность сделать выбор между различными вариантами конфигурации среды облачных вычислений и выбрать наиболее приемлемый вариант с точки зрения требований безопасности.

ЛИТЕРАТУРА

1. Accorsi R., Wonnemann C. Auditing Workflow Execution against Dataflow Policies. – In Proc. BIS, 2010. – pp. 207–217.

2. Bell D. E., LaPadula L. J. Secure Computer System: Unified Exposition and Multics Interpretation. – Tech report ESD-TR-75-306, Mitre Corp, Bedford, Ma, 1976.

3. Bishop M. Computer Security: Art and Science. – Boston: Addison-Wesley Professional. 2002. – 1084 p.

4. Вдовин И. COBIT 4.1. – М.: Аудит и контроль информационных систем, 2008. – 240 с.

5. Mell P., Tim Grance T. The NIST Definition of Cloud Computing [Электронный ресурс]. – Режим доступа: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

6. NVD Common Vulnerability Scoring System Support v.2. [Электронный ресурс]. – Режим доступа: http://nvd.nist.gov/cvss.cfm?calculator&version=2.

7. Trope R. L. [and other] A Coherent Strategy for Data Security through Data Governance // Data Governance. – 2007. – Vol. 5. – No. 3. – pp. 32–39.

8. Волков С. Д., Царегородцев А. В., Цацкина Е. П. Особенности построения систем обнаружения компьютерных атак для информационно-телекоммуникационных систем, функционирующих на основе технологии облачных вычислений [Электронный ресурс] // Огарев-online. – 2017. – №13. – Режим доступа: http://journal.mrsu.ru/arts/osobennosti-postroeniya-sistem-obnaruzheniya-kompyuternyx-atak-dlya-informacionno-telekommunikacionnyx-sistem-funkcioniruyushhix-na-osnove-texnologii-oblachnyx-vychislenij.

9. Царегородцев А. В., Качко А. К. Обеспечение информационной безопасности на облачной архитектуре организации // Национальная безопасность. – 2011. – № 5. – С. 25–34.

10. Царегородцев А. В., Качко А. К. Один из подходов к управлению информационной безопасностью при разработке информационной инфраструктуры организации // Национальная безопасность. – 2012. – № 1(18). – С. 46–59.